CCN-CERT

BP/10

Recomendaciones de seguridad para CDN

INFORME DE BUENAS PRÁCTICAS

FEBRERO 2022

ccn-cert centro criptológico nacional
CCN centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Pº de la Castellana 109, 28046 Madrid

Fecha de edición: junio de 2022

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Índice

1. Sobre CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015, de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas del Sector público,** a **empresas y organizaciones de interés estratégico** para el país y a cualquier sistema clasificado. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN.

2. Introducción a los CDN

Las redes de distribución de contenido (CDN) son elementos de gran valor, encargados de la entrega de diversos contenidos con los que el usuario interactúa a diario. Este tipo de arquitecturas surgieron para resolver, principalmente, un problema de latencia, entendida como la demora ocurrida entre el momento de solicitar un sitio web hasta el momento que este contenido se entrega y muestra por pantalla.

En este proceso influyen una serie de factores, muchos de ellos específicos del tipo de contenido, servidor y sitio web solicitado, siendo el más importante la distancia física entre el usuario y el servidor que aloja el contenido.

Este tipo de arquitecturas surgieron para resolver el problema de la latencia.

2. Introducción a los CDN

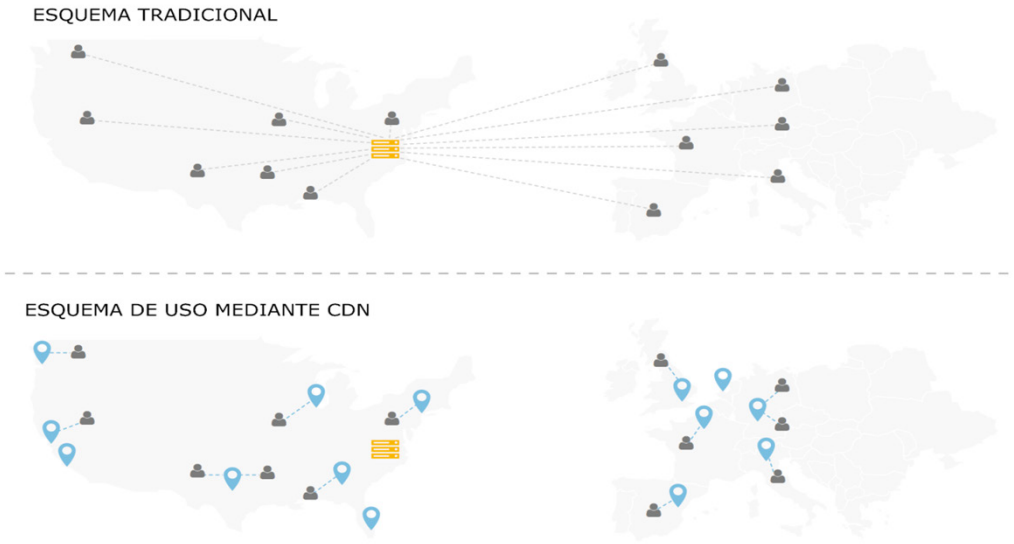

Figura 1 - Esquema de funcionamiento de una red CDN

La misión principal de un CDN es reducir virtualmente esa distancia física, con el objetivo de mejorar la velocidad y el rendimiento. Para ello, un CDN almacena en caché una versión del contenido a servir en múltiples ubicaciones geográficas, conocidas como Puntos de Presencia o PoP (*Points of Presence*). Cada uno de estos PoP contiene una serie de servidores de almacenamiento responsables de la entrega de contenido a los visitantes que se encuentren geográficamente cerca.

Además de esta optimización en términos de latencia, una red CDN proporciona otra serie de ventajas:

- Aumenta la velocidad de carga de un sitio web.
- Bloquea *bots, spammers* y otro tipo de herramientas dañinas.
- Reduce el consumo de ancho de banda.
- Permite balancear la carga entre diferentes servidores.
- Protege a los sitios web de ataques distribuidos de denegación de servicio (DDoS).
- Incrementa el nivel de seguridad a través de diferentes reglas y mecanismos de protección.

2. Introducción a los CDN

Para que estos mecanismos sean aplicables, como normal general, será necesario modificar el servidor raíz DNS del dominio (ej.: midominio.com). En esencia, se necesitará modificar el registro A principal del DNS para que apunte a una dirección IP específica del rango del CDN, aunque también existen proveedores que permiten realizar la implementación a nivel de CNAME sin necesidad de modificar el servidor DNS raíz. En ambos casos, el usuario final será redirigido a la red CDN en lugar de al servidor de origen.

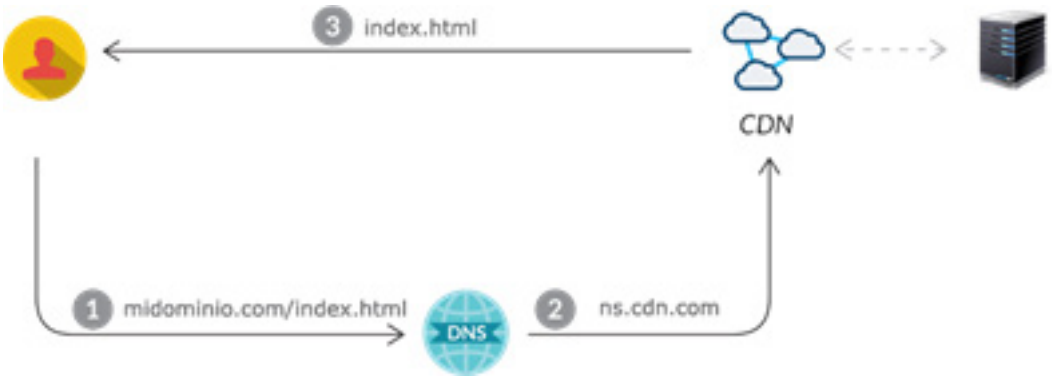

Figura 2 - Interactuación del usuario y la red CDN

Existe un gran número de proveedores de servicio de CDN, con versiones tanto gratuitas como de pago. En este guía se proporcionarán recomendaciones genéricas para cualquiera de ellos.

3. Comparativa general de los principales proveedores de CDN

	CLOUDFLARE	Incapsula	Akamai
PoPs (puntos de presencia)	120	42	2200
Tiempo mínimo de contratación (meses)	1	1	12
Panel de control online	✓	✓	✓
Alta online	✓	✓	✗
Soporte CNAME	✓	✓	✓
Soporte SPYDY	✗	✗	✓
Soporte HTTP/2	✓	✓	✓
Soporte IPV6	✓	✓	✓
Compresión GZIP	✓	✓	✓
Protección DDOS	✓	✓	✓
WAF	✓	✓	✓
Control de acceso por IP	✓	✓	✓

3. Comparativa general de los principales proveedores de CDN

	CLOUDFLARE	Incapsula	Akamai
Certificado SSL propios	✓	✓	✓
Uso de API	✓	✓	✓
Acceso a logs formato RAW	✓	✗	✓
Video bajo demanda (VOD)	✗	✗	✓
Opciones de almacenamiento	✗	✗	✓
Estadísticas en tiempo real	✓	✓	✓

4. Técnicas de protección de los CDN frente a ataques DDOS

Un ataque distribuido de denegación de servicio (DDoS) es un tipo de ataque cuya finalidad es hacer que un servicio en línea no esté disponible, generalmente interrumpiendo o suspendiendo temporalmente los servicios que presta el servidor. Los ataques se originan desde dispositivos comprometidos, ya sean equipos personales, routers o dispositivos IoT, a menudo distribuidos globalmente en lo que se conoce como botnet.

Estas agresiones se diferencian de un ataque convencional de denegación de servicio (DoS), ya que éste sólo utilizaría un solo dispositivo conectado a Internet (una conexión de red) para inundar un objetivo con tráfico dañino.

Un ataque DDoS es un tipo de ataque cuya finalidad es hacer que un servicio en línea no esté disponible, generalmente interrumpiendo o suspendiendo los servicios que presta el servidor.

4. Técnicas de protección de los CDN frente a ataques DDOS

Una vez que el atacante posee el control de una *botnet*, puede controlar las máquinas enviando instrucciones actualizadas a cada *bot* a través de un panel de control remoto. Cuando la *botnet* apunta a la dirección IP de una víctima, cada *bot* responderá enviando solicitudes al objetivo, lo que podría ocasionar que el servidor o la red objetivo superase su capacidad de respuesta, provocando una degradación del servicio, que podría incluso acabar con una interrupción indefinida del mismo.

Debido a que cada *bot* es un dispositivo legítimo de Internet, separar el tráfico dañino del tráfico legítimo no es una tarea sencilla.

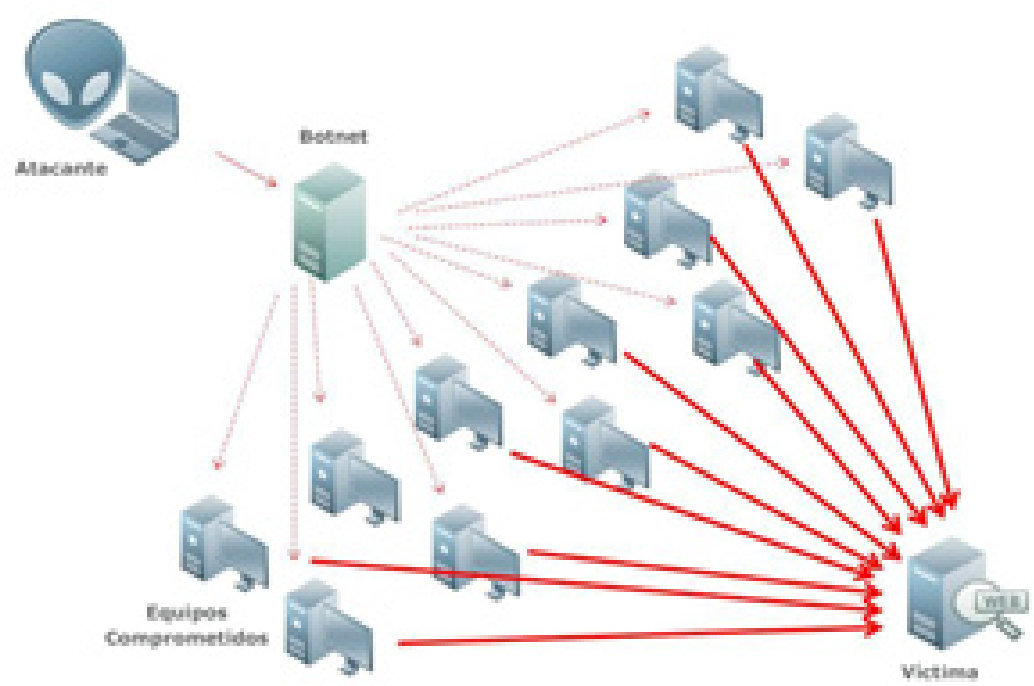

Figura 3 - Esquema de funcionamiento de una botnet

4. Técnicas de protección de los CDN frente a ataques DDOS

En términos generales, los ataques DoS y DDoS se pueden dividir en tres (3) tipos:

- **Ataques volumétricos:** incluye inundaciones UDP, inundaciones ICMP y otras inundaciones provocadas por paquetes generados de manera artificial. El objetivo del ataque es saturar el ancho de banda del sitio atacado, y se mide en bits por segundo (bps).
- **Ataques a nivel de protocolo:** incluye inundaciones SYN, ataques de paquetes fragmentados, etc. Este tipo de ataques consume recursos reales del servidor o de equipos de comunicación intermedios como cortafuegos y balanceadores de carga, y se mide en paquetes por segundo (pps).
- **Ataques a nivel 7 (en la capa de aplicación):** incluye ataques como *slowloris*, inundaciones GET/POST y ataques dirigidos a vulnerabilidades de servidores Apache entre otros. Generalmente, se utilizan solicitudes aparentemente legítimas y el objetivo de estos ataques es bloquear el servidor web. Se miden en solicitudes por segundo (rps).

Los atacantes están motivados principalmente por:

- **Ideología:** los llamados "hacktivistas" usan ataques DDoS como un medio para agredir sitios web con los que no están de acuerdo ideológicamente.
- **Conflictos empresariales:** las empresas pueden usar ataques DDoS para eliminar estratégicamente los sitios web de los competidores, por ejemplo, para evitar que participen en un evento significativo (por ejemplo, en el Black Friday).
- **Vandalismo:** "script-kiddies" usan herramientas públicas disponibles en Internet para lanzar ataques de DDoS sin una motivación clara o sin la intención real de obtener un beneficio a cambio.
- **Extorsión:** los atacantes usan ataques DDoS o la amenaza de llevarlos a cabo como medio para extorsionar y obtener dinero de sus víctimas.
- **Guerra digital:** los ataques DDoS autorizados por un gobierno pueden usarse contra la infraestructura de un país enemigo.

La mitigación de un ataque DDoS requiere una estrategia en función del tipo de ataque, y si es de uno o varios tipos al mismo tiempo. En términos generales, cuanto más complejo es el ataque, más difícil es identificar tráfico dañino ya que el objetivo del atacante es aparentar tráfico legítimo haciendo que la mitigación sea lo menos eficiente posible.

Por este motivo, **prácticamente la totalidad de los servicios de CDN ofrecen servicios para mitigar este tipo de ataques.** En función del nivel de seguridad que el usuario haya seleccionado, normalmente *Bajo, Medio* o *Alto Ataque*, el CDN analizará y filtrará las conexiones, implementando una serie de medidas de seguridad adicionales para realizar filtrado de tráfico.

4.1 Javascript challenges

Es un tipo de desafío que se utiliza para filtrar a los atacantes, que utilizan herramientas automatizadas, de los clientes legítimos. El desafío se basa en enviar a cada cliente, atacante o usuario legítimo, un código *JavaScript* que incluya algún tipo de reto. Prácticamente cualquier navegador en la actualidad tiene un motor *JavaScript* y fácilmente entenderá y resolverá el desafío de forma transparente (sin interacción del usuario), mientras que las herramientas automatizadas de DDoS normalmente no están equipadas con este tipo de funcionalidades *JavaScript* y, por lo tanto, no podrán superar el desafío ni establecer la conexión con el servidor final.

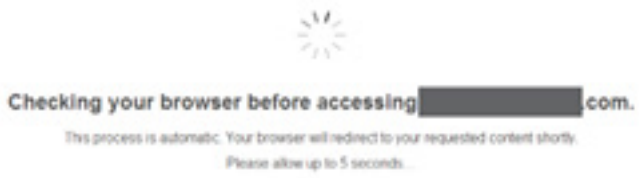

Figura 4 - Desafío JavaScript proporcionado por CloudFlare

4.2 Pruebas en paquetes TCP SYN

Con este método, se trata de comprobar que la pila TCP del cliente es válida y se encuentra correctamente implementada, buscando una respuesta correcta a ciertos paquetes construidos bajo condiciones fuera de lo normal, permitiendo detectar paquetes desde direcciones IP de origen falsas y paquetes generados mediante sockets utilizando una herramienta de DDoS.

Dentro de las tácticas más comunes podemos encontrar desde devolver un paquete RST en el primer SYN recibido (esperando que el cliente lo vuelva a reenviar) hasta enviar deliberadamente un SYN-ACK con un número de secuencia incorrecto esperando que el cliente devuelva un RST y que luego vuelva a intentarlo.

La forma más sencilla para responder a esta tipología de pruebas es permitir que sea el sistema operativo el que responda a estos paquetes, haciéndola efectiva cuando se trata de una conexión legítima.

Principalmente existen dos (2) técnicas:

a. **TCP Reset:** el CDN enviará un paquete con el *flag* de RESET (RST) activo para restablecer las conexiones TCP establecidas (las que han completado satisfactoriamente el *handshake*). Es el método más común de verificación, ya que las herramientas y *bots* para DDoS diseñados no tienen esta lógica implementada, a diferencia de una conexión a través de un navegador real.

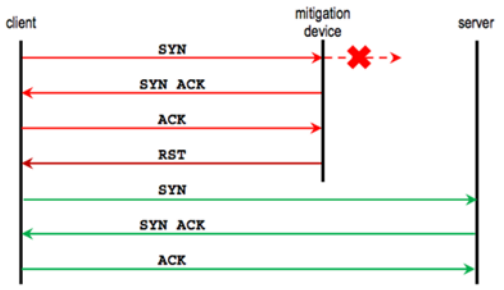

Figura 5 - Funcionamiento de la mitigación por TCP Reset

b. **TCP out-of-sequence:** a diferencia del método anterior, el CDN puede deliberadamente plantear un desafío al cliente enviando respuestas SYN-ACK con un número fuera de la secuencia como se ve en la figura a continuación. Dado que el número de secuencia es incorrecto, se supone que el cliente restablece la conexión TCP y establece la conexión de nuevo. De nuevo, un bot o una herramienta DDoS no resolvería estos casos.

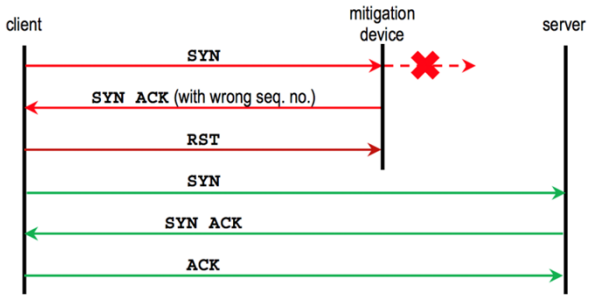

Figura 6 - Funcionamiento de la mitigación por TCP out-of-sequence

4.3 Filtrado de conexiones SSL

Hoy en día, debido al incremento de las medidas de seguridad frente a las técnicas DDoS convencionales, se comienza a ver un incremento en las inundaciones dañinas de conexiones SSL.

Estas inundaciones SSL evitan gran cantidad de dispositivos de seguridad, como cortafuegos o sistemas de protección frente a intrusiones (IPS). Además, existen variantes actuales como ataques de renegociación SSL, donde a diferencia de los ataques tradicionales, el atacante necesita sólo una décima parte de la potencia de cómputo del servidor desprotegido para acabar con sus recursos e interrumpir el tráfico legítimo a estos.

Un proveedor de CDN simplemente elimina conexiones SSL vacías o dañinas, protegiendo los recursos que se encuentren detrás de las mismas.

4.4 Redirección 302 HTTP

La idea básica es que un navegador legítimo respetará las redirecciones HTTP 302. Por este motivo, se prueba a insertar redirecciones generadas de forma dinámica para asegurar que el visitante es un usuario legítimo, que puede interpretar estas acciones mediante el navegador.

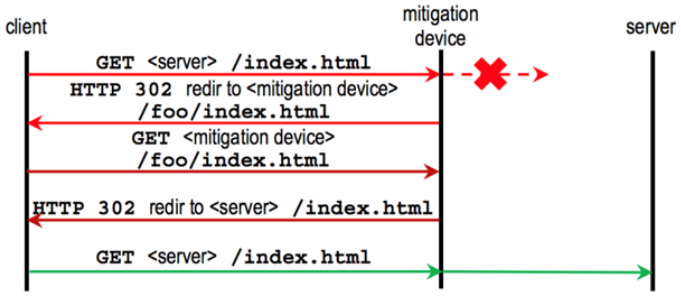

Figura 7 - Funcionamiento de la mitigación por redirección HTTP

4.5 Cookies HTTP

Esta técnica generalmente va enlazada con la anterior y permite identificar el tráfico malicioso al inyectar de forma dinámica una cookie en la conexión entre el supuesto cliente legítimo y el CDN. Aquel tráfico que no sea capaz de interpretar esta nueva situación, por tratarse probablemente de tráfico dañino, será descartado.

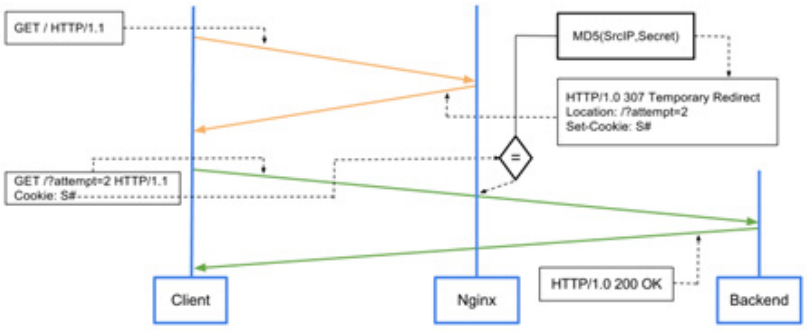

Figura 8 - Funcionamiento de la mitigación HTTP cookies en un módulo de Nginx

4.6 CAPTCHA

Un CAPTCHA *(Completely Automated Public Turing test to tell Computers and Humans Apart)* es una prueba desafío-respuesta utilizada para determinar cuando el usuario es o no humano.

Esta técnica es probablemente la más extendida, sencilla y segura de utilizar ya que implica la intervención humana directa. Si el cliente tiene éxito al resolverlo, se mantendrá en la lista blanca durante un cierto tiempo o para cierta cantidad de tráfico, después de lo cual deberá de autenticarse de nuevo.

Figura 9 - Ejemplo de funcionamiento de un sistema desafío-respuesta basado en CAPTCHA

Este método es, en sí mismo, bastante intrusivo y en la práctica se usa generalmente al configurar el CDN en modo *Bajo Ataque*.

5. Recomendaciones de seguridad en el uso de CDN

5.1 Configurar SSL/TLS en la conexión entre el usuario y el CDN

En la medida de lo posible debe utilizarse la comunicación SSL/TLS entre el CDN y el servidor de origen. *Transport Layer Security* (TLS) es un protocolo de cifrado de datos enviados por Internet, que surgió del *Secure Sockets Layer* (SSL), con el fin de corregir la mayoría de fallos de seguridad de este protocolo (la industria aún utiliza estos términos de manera intercambiable por razones históricas).

De esta forma TLS está diseñado para proveer:

Autenticación

Cifrado

Integridad

Para poder realizar la activación de TLS sobre la configuración, el sitio web necesitará un certificado SSL y su clave privada correspondiente. Existen una serie de herramientas, así como una metodología de evaluación sencilla, que permiten a los administradores evaluar la configuración del servidor SSL donde se tienen en cuenta factores tales como que el certificado sea válido y de confianza, el soporte de protocolos, intercambio de claves y soporte de cifrado.

Combinando la puntuación de estas pruebas, con una puntuación entre 0 y 100, se obtiene una puntuación global que se convierte en una letra, de la A (mayor puntuación) a la F (menor puntuación).

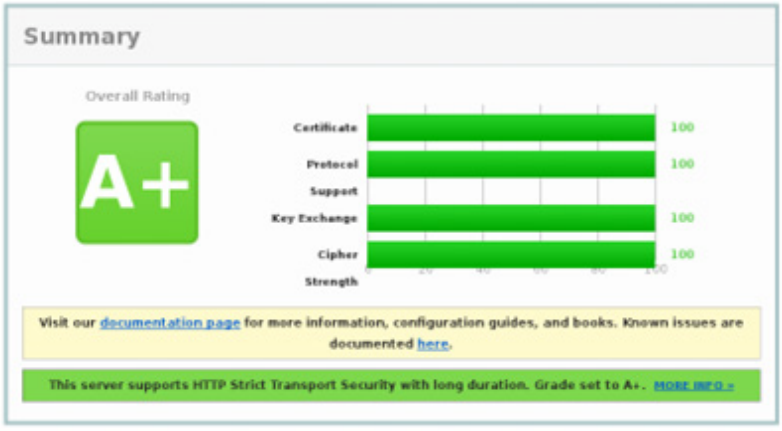

Figura 10.- Ejemplo de puntuación de la herramienta SSL Server Test de Qualys

Activar SSL/TLS sobre la configuración del CDN tiene el beneficio de proporcionar seguridad a los visitantes utilizando un certificado generado por él mismo.

Debido a que los visitantes se conectan solamente al CDN, un certificado menos seguro (por ejemplo, puntuado con la letra C) que esté en uso entre el servidor de origen y el CDN no afectará a esta experiencia, ya que probablemente el ofrecido por el CDN obtendrá una puntuación mayor, sin necesidad de modificar la configuración en el servidor de origen.

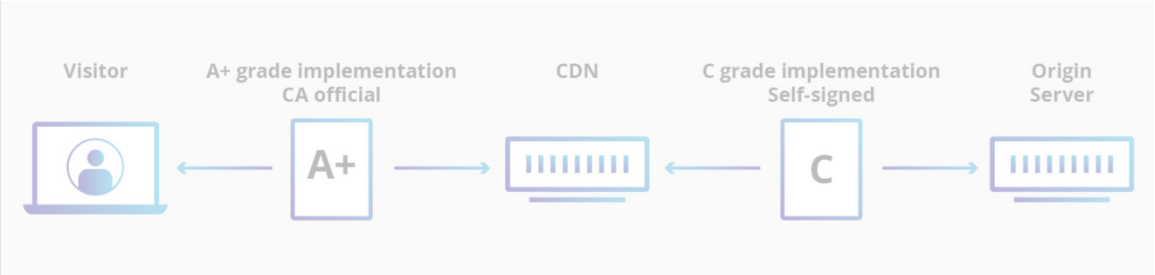

Figura 11.- Implementación y securización de certificado CDN

5.2 Configuración para servicios bajo conexión

Existen algunos casos en los que el servidor de origen no está configurado para ofrecer conexiones seguras bajo SSL, ya sea por su incorrecta administración o porque se trata de un servicio que no es posible configurar de forma segura.

En estos casos será necesario configurar la conexión del CDN sobre SSL para el tráfico entre éste y los visitantes, mientras que la conexión entre el CDN y el sitio web se mantiene sobre http sin necesidad de realizar ninguna configuración adicional sobre el servidor web de origen.

Además, debemos tener en cuenta que la falta de implementación de SSL puede tener resultados negativos en otro tipo de aspectos, como en el posicionamiento de algunos buscadores como Google.

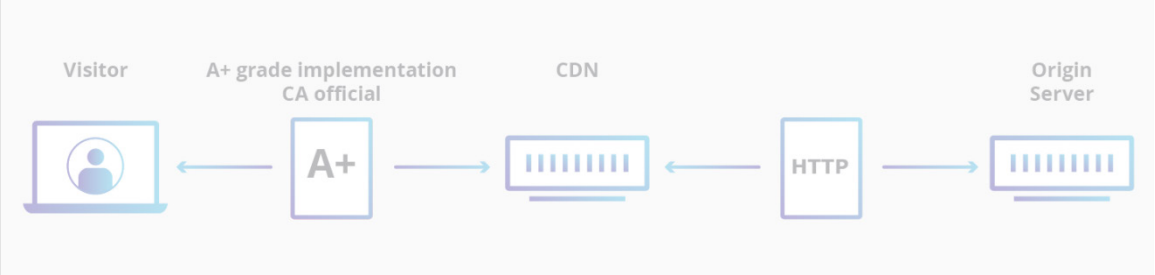

Figura 12.- Implementación de SSL en servidores http

Adicionalmente, el propio CDN se encargará de elegir los algoritmos de cifrado más seguros, independientemente de la configuración del sitio web, así como implementar otras opciones como *Forward Secrecy*.

5.3 Activar el uso de HSTS

HSTS (por sus siglas *HTTP Strict Transport Security*) es una tecnología de políticas de seguridad web, diseñadas para ayudar a proteger servidores HTTPS contra ataques de degradación.

Este tipo de ataques de degradación (conocidos como *SSL stripping attacks*) permiten realizar ataques MiTM (Man-in-the-middle) donde un posible atacante podría redirigir el navegador desde un servidor web HTTPS correctamente configurado a un servidor propio a través de un canal HTTP. Una vez se ha logrado esta redirección, los datos intercambiados, como cookies, pueden verse comprometidos.

Entre los navegadores que soportan HSTS se encuentran:

Google Chrome desde la versión 4.0.211.0.

Google Chrome para Android desde la versión 18.

Firefox y Firefox Mobile desde la versión 4.

Opera desde la versión 12.

Safari desde la versión 7.

Android Browser desde la versión 4.4 de Android.

Internet Explorer planea implementarlo en la versión 12 de su navegador.

La mayoría de los CDN permiten configurar y activar esta opción, añadiendo cabeceras donde se puede definir la duración de esta política, incluir diferentes subdominios, etc.

5.4 Uso de certificado de cliente

TLS (la versión moderna de SSL) permite a un cliente verificar la identidad del servidor con el que está realizando la conexión. Normalmente, un *handshake* de TLS es unidireccional, es decir, el cliente puede verificar la identidad del servidor, pero el servidor no puede verificar la identidad del cliente. En un *handshake* de TLS autenticado por el cliente, ambos lados proporcionan un certificado para verificar su identidad.

Si el servidor de origen está configurado para aceptar solicitudes que usan un certificado de cliente válido del CDN, el tráfico que no pase a través de la red de éste será descartado al no disponer del certificado correcto.

Esto significa que los atacantes no pueden eludir las características del CDN, como el WAF, las reglas para el límite de conexiones o la protección frente a ataques DDoS. Incluso en el caso en el que un posible atacante lograra falsear la dirección IP de origen, suplantando cualquier dirección IP del pool del CDN, no podría establecer una conexión con el servidor final.

Por lo tanto, implantar y configurar el certificado de cliente del proveedor de CDN añadirá un nuevo nivel de seguridad al servicio web, además de evitar posibles fugas de información y eliminar gran parte del riesgo de las herramientas de escaneo masivo.

5.5 Cambiar la dirección IP original asociada al servidor

Si el sitio web no se configuró inicialmente con el CDN, puede haber existido un período en el que el DNS apuntara directamente a la dirección IP de origen. Con el uso de herramientas disponibles online es posible consultar fácilmente el historial de los registros DNS, que pueden revelar las direcciones IP en uso antes de que se activara el CDN y que aún pueden estar siendo utilizadas para el mismo propósito.

Este riesgo no puede mitigarse de forma directa, ya que la información disponible es histórica. Sin embargo, siempre puede solicitarse una nueva dirección IP de un rango diferente al que se hubiera mantenido durante la implantación del CDN.

A continuación, se muestra un ejemplo de una de estas herramientas que muestra la información histórica que mantiene.

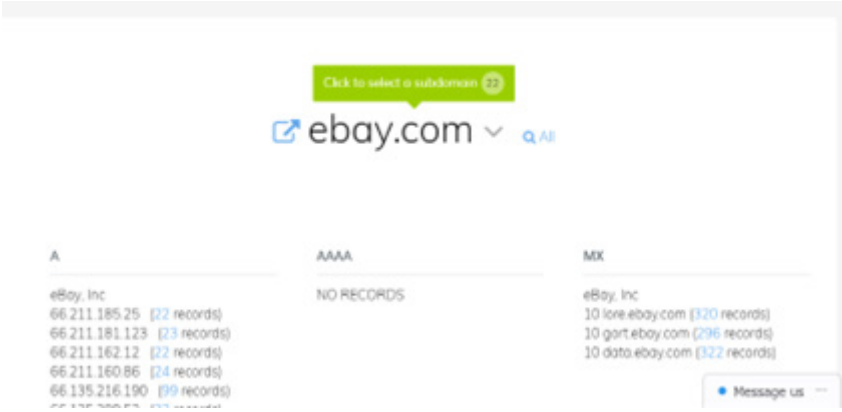

Figura 13 - Obtención de información histórica de un dominio

5.6 Permitir sólo el acceso al pool de direcciones IP del CDN

Una de las tareas principales a realizar cuando se implementa un CDN es incluir todas las direcciones IP especificadas por el proveedor en una lista blanca que permita las conexiones, bloqueando cualquier otro tipo de petición externa.

Esto debe realizarse tanto a nivel IPv4 como a nivel IPv6, en caso de ser utilizado, y en el caso de Linux se podrá utilizar *iptables* para realizarlo de forma sencilla. Por ejemplo, para permitir la conexión desde la dirección IP 1.1.1.1 se puede ejecutar el siguiente comando:

```
$ iptables -I INPUT -p tcp -m multiport --dports http,https -s “1.1.1.1”
-j ACCEPT
```

Después se añadirá una regla final para bloquear cualquier intento de conexión desde direcciones IP que no hayan sido especificadas con el comando anterior:

```
$ iptables -I INPUT -p tcp -m multiport --dports http,https -j DROP
```

Se deberá tener en cuenta que, en función del sistema operativo utilizado, será necesario también guardar esta tabla para recuperarla en caso de reinicio del sistema. En el caso de sistemas Linux es posible salvar el estado de las reglas de *iptables* con los siguientes comandos.

- **Debian/Ubuntu:** iptables-save > /etc/iptables/rules.v4
- **RHEL/CentOS:** iptables-save > /etc/sysconfig/iptables
- **Debian/Ubuntu:** ip6tables-save > /etc/iptables/rules.v6
- **RHEL/CentOS:** ip6tables-save > /etc/sysconfig/ip6tables

5.7 Proteger contra ataques de fuerza bruta y límite de conexiones

Otra característica de gran utilidad de los CDN es que permiten al administrador establecer límites de conexiones para proteger el sitio web ante ataques de denegación de servicio, intentos de inicio de sesión por fuerza bruta contra un panel de acceso o administración, así como otro tipo de comportamientos abusivos dirigidos a la capa de aplicación.

Figura 14 - Funcionamiento de un ataque de fuerza bruta

Generalmente, los módulos de inicio de sesión se realizan a través de peticiones POST donde se envía un nombre de usuario y contraseña al servidor web. Durante la preparación de un ataque de fuerza bruta, un atacante captura estas peticiones de acceso y las utiliza para generar un ataque automatizado, lanzando peticiones de forma consecutiva, al mayor ritmo posible, con el fin de obtener una combinación válida de usuario y contraseña que le permita el acceso.

Se podrá, por ejemplo, configurar el sistema para prevenir que un posible atacante realice un ataque de fuerza bruta contra el panel de administración de un sitio Wordpress, generando un bloqueo al llegar a cierto número de intentos fallidos o de forma genérica al detectar un error tipo 401 (acceso no autorizado) o 403 (acceso prohibido), detectar un crawler o bot dañino y generar una acción cuando por ejemplo realice accesos a páginas no encontradas (códigos 404), etc.

Esta limitación, de forma más general, permite establecer umbrales de tiempo, definir el tipo de respuesta sobre URL específicas del sitio web, reduciendo incluso el ancho de banda utilizado y protegiendo al servidor final.

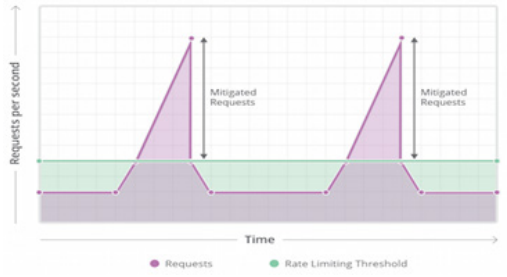

Figura 15 - Funcionamiento de Rate Limiting

5.8 Revisar la configuración de los registros DNS

Ninguno de los registros DNS debe contener alguna mención de la dirección IP de origen. Deben revisarse de forma exhaustiva los siguientes registros DNS para asegurarse de que no contengan ninguna información sobre el origen:

SPF: SPF (el acrónimo de Sender Policy Framework) es una protección contra la falsificación de direcciones en el envío de correos electrónicos. Identifica a los servidores de correo SMTP autorizados para el transporte de los mensajes a través de los registros DNS.

TXT: un registro TXT es un tipo de registro DNS que contiene información de texto de fuentes externas a un dominio y que se añade a la configuración de éste.

Además, deberá tenerse especial atención en la configuración del resto de subdominios alojados, ya que alguno de estos podría encontrarse aún configurado de forma directa a la dirección IP del servidor de origen, exponiendo ésta a posibles atacantes y anulando la mitigación del CDN frente a diferentes ataques.

5.9 Alojar el correo en un servidor diferente

Si el servidor de correo está alojado en la misma dirección IP que el servidor web de origen, un atacante podría encontrar la dirección IP en un correo electrónico saliente.

Por ejemplo, un atacante podría enviar un correo a una dirección inexistente para generar un rebote, donde la dirección IP de origen del servidor podría ser expuesta en las cabeceras (el rebote puede contener la dirección IP de su servidor en alguno de sus campos).

Existen, incluso, casos en los que no es necesario el envío de un correo si la plataforma, por ejemplo, dispone de un sistema de registro de usuarios o para obtener la contraseña en caso de que el usuario la haya olvidado.

Además, los registros MX siempre muestran el servidor de correo real. Por lo tanto, si el correo de un dominio pasa por el mismo servidor web, podrá encontrarse fácilmente la dirección IP a través de los registros MX.

La siguiente imagen muestra un ejemplo, donde la dirección IP real del servidor (52.x.x.x) ha quedado expuesta mediante el empleo del correo electrónico:

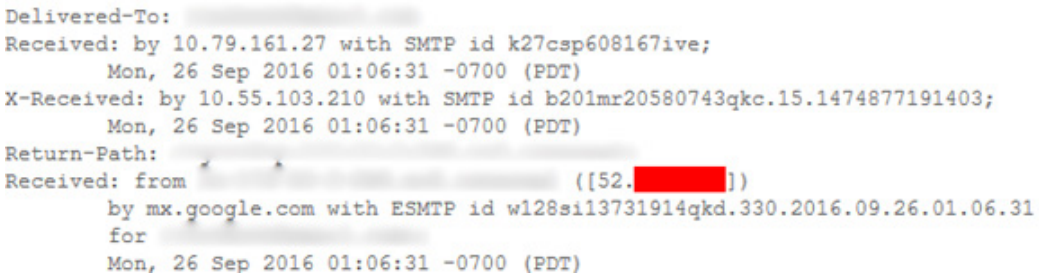

Figura 16 - Descubrimiento de IP de origen a través del servicio de correo

Otra opción para evitar este tipo de fugas de información sería utilizar el servicio a través de un tercero para enviar los correos en nombre del dominio propio.

5.10 Deshabilitar la inclusión dinámica de ficheros

Una gran cantidad de servicios web le ofrecen al usuario la opción de establecer, por ejemplo, una imagen personalizada como avatar de usuarios. En la mayoría de los casos, ofrecen la posibilidad no sólo de cargar directamente una imagen en el servidor, sino también de proporcionar una URL remota desde la cual recuperar la imagen.

Si el servidor descarga este archivo, esto abre la opción para un nuevo vector de ataque, permitiendo a un posible atacante obtener la dirección IP real de forma sencilla.

Con algunas líneas de PHP y un fichero *.htaccess* correctamente elegido, es posible crear un enlace a un recurso (por ejemplo, una imagen) que registra la dirección IP de cualquiera que intente recuperarla:

```
# Contenido de .htaccess
AddHandler application/x-httpd-php5 .jpg

# Fichero de ejemplo fichero.php
    <?php

    $fh =@fopen("log.txt", "a+");
    $timestamp = date('l jS \of F Y h:i:s A');
    $hostname = @gethostbyaddr($_SERVER['REMOTE_ADDR']);

    @fwrite($fh, "\r\n$timestamp\r\n");
    @fwrite($fh, 'REMOTE_ADDR: '.$_SERVER['REMOTE_ADDR']."\r\n");
    @fwrite($fh, 'Host Name: '."$hostname\r\n");
    @fwrite($fh, 'HTTP_CLIENT_IP: '.$_SERVER['HTTP_CLIENT_IP']."\r\n");
    @fwrite($fh, 'HTTP_USER_AGENT: '.$_SERVER['HTTP_USER_AGENT']."\r\n");

    fclose($fh);
    // bait.png is the image to show when grabbing the ip
    // give 755 permissions to bait.png
    $im = imagecreatefrompng("bait.png");
    header('Content-Type: image/jpeg');
    imagepng($im);
    imagedestroy($im);
    ?>
```

Un posible atacante podría utilizar otra serie de servicios online para lograr la misma finalidad, sin la necesidad de disponer de un servidor web propio, con los mismos resultados e incluso con un nivel de anonimato aún mayor.

5.11 Configurar WAF y protección a nivel aplicación

En algunos casos, los atacantes usan ataques de DDoS para debilitar las defensas del perímetro o bloquear los dispositivos de seguridad. Por esta causa, muchos CDN proporcionan la posibilidad de utilizar un sistema WAF (*Web Application Firewall)*, que protegerá al cliente de una gran cantidad de ataques.

Un cortafuegos de aplicaciones web es un cortafuegos que supervisa la seguridad web y filtra o bloquea el tráfico hacia y desde una aplicación web. De esta manera, puede filtrar el contenido de aplicaciones web, mientras un cortafuegos de red protege el tráfico solamente entre los servidores.

Por norma general, en un WAF se encontrarán las reglas que son de aplicación para las 10 vulnerabilidades principales OWASP:

- **Inyección.**
- **Autentificación y gestión de sesiones.**
- **Cross-Site Scripting (XSS).**
- **Referencias inseguras a objetos.**
- **Configuración débil de seguridad.**
- **Filtración de información confidencial.**
- **Falta de control en el acceso.**
- **Falsificación de petición en sitios cruzados (CSRF).**

Usar componentes con vulnerabilidades conocidas.

Redirecciones y envíos no validados. Usar componentes con vulnerabilidades conocidas.

Además, deberá tenerse especial atención en la configuración del resto de subdominios alojados, ya que alguno de estos podría encontrarse aún configurado de forma directa a la dirección IP del servidor de origen, exponiendo ésta a posibles atacantes y anulando la mitigación del CDN frente a diferentes ataques.

Figura 17 - Sistema de protección WAF basado en CDN

5.12 Evitar los motores de búsqueda de servicios

Existen gran cantidad de herramientas de búsquedas de servicios y servidores disponibles de forma online que pueden permitir el acceso a la información de la dirección IP de origen del nuevo servicio configurado.

Una de las más conocidas es **Shodan**, un motor de búsqueda que permite al usuario a través de una variedad de filtros encontrar equipos específicos (routers, servidores, etc.) conectados a Internet. También puede entenderse como un motor de búsqueda de banners de servicio, que son metadatos que el servidor envía de vuelta al cliente.

Esta información puede contener versiones del software de servidor, que opciones admite el servicio, un mensaje de bienvenida o cualquier otra cosa que el cliente pueda conocer antes de interactuar con el servidor y que puede utilizarse para localizar el servidor de origen que se encuentra detrás de un servicio de CDN.

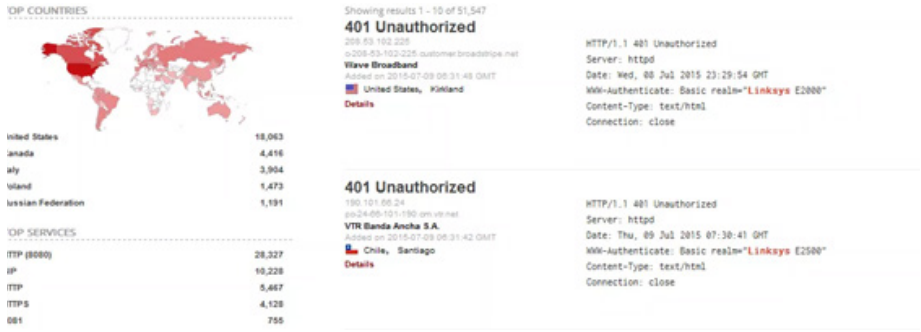

Figura 18 - Ejemplo de búsqueda en Shodan

Otro servicio muy utilizando es **Censys**, que recopila datos de servidores, servicios y sitios web a diario, escaneando todo el espectro de direcciones IPv4. Por ejemplo, sabiendo que el dominio moz.com se encuentra protegido por un CDN, se puede realizar una búsqueda en Censys para intentar obtener mayor información, obteniendo lo siguiente:

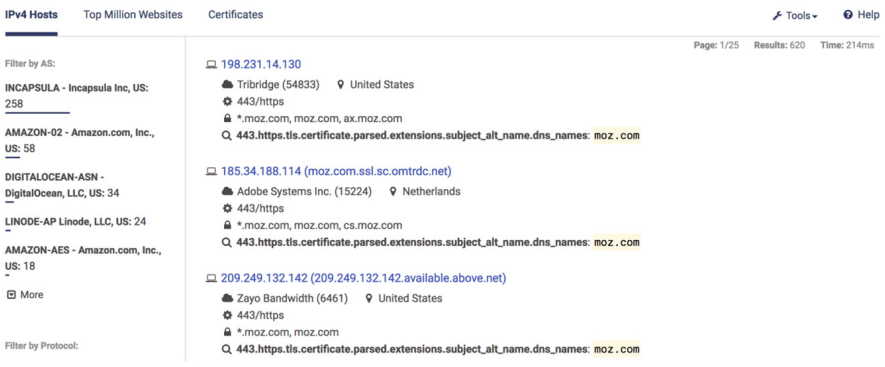

Figura 18 - Ejemplo de búsqueda en Shodan

Como se aprecia en la captura, existen gran cantidad de campos que pueden utilizarse para realizar estas búsquedas, como CN (Common Name), SAN (Subject Alternative Name), el cómputo SHA256 del certificado, el código de respuesta HTTP (en este caso 200), etc. hasta averiguar la dirección IP de origen del dominio, que en este caso pertenecen al rango 209.249.132.0/24.

6. Decálogo básico de seguridad

Este decálogo de buenas prácticas pretende sentar las bases sobre las medidas de seguridad a tener en cuenta cuando se migra un servicio a un proveedor de CDN.

Decálogo de recomendaciones

1. Configuración de SSL/TLS, incluyendo HSTS, en la conexión entre el usuario final y el CDN.
2. Utilizar certificados de cliente entre el CDN y el servidor de origen.
3. Modificar la dirección IP del servidor de origen si ha sido expuesta anteriormente.
4. Permitir sólo acceso al servidor de origen por una dirección IP del pool del CDN.
5. Proteger el servicio web contra ataques de fuerza bruta e implementar la limitación del número de conexiones del cliente.
6. Revisar la configuración de los registros DNS.
7. Migrar el servicio de correo electrónico en caso necesario.
8. Deshabilitar, si existe, la inclusión dinámica de ficheros en el servicio web correspondiente.
9. Disponer de un WAF e implementar medidas de seguridad a nivel aplicación.
10. Comprobar que los datos del servidor de origen no se encuentren en motores de búsqueda de Internet como Shodan o Censys.

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

Referencias

- http://hopandfork.org/2016/11/16/cloudflare-ip-unveil.html
- https://www.defcon.org/images/defcon-21/dc-21-presentations/Mui-Lee/DEFCON-21-Miu-Lee-Kill-em-All-DDoS-Protection-Total-Annihilation-WP-Updated.pdf

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es